

# WAFOM on abelian groups for quasi-Monte Carlo point sets \*

Kosuke Suzuki<sup>†</sup>

March 31, 2014

## Abstract

In this paper, we study quasi-Monte Carlo (QMC) rules for numerical integration. J. Dick proved a Koksma-Hlawka type inequality for  $\alpha$ -smooth integrands and gave an explicit construction of QMC rules achieving the optimal rate of convergence in that function class. From this inequality, Matsumoto et al. introduced Walsh figure of merit (WAFOM)  $WF(P)$  for an  $\mathbb{F}_2$ -digital net  $P$  as a quickly computable quality criterion for  $P$  as a QMC point set. The key ingredient for obtaining WAFOM is the Dick weight, a generalization of the Hamming weight and the Niederreiter-Rosenbloom-Tsfasman (NRT) weight.

We extend the notions of the Dick weight and WAFOM for digital nets over a general finite abelian group  $G$ , and show that this version of WAFOM satisfies Koksma-Hlawka type inequality when  $G$  is cyclic. We give a MacWilliams-type identity on the weight enumerator polynomials for the Dick weight, by which we can compute the minimum Dick weight as well as WAFOM. We give a lower bound of WAFOM of order  $N^{-C'_G(\log N)/s}$  and an upper bound of lowest WAFOM of order  $N^{-C_G(\log N)/s}$  for given  $(G, N, s)$  if  $(\log N)/s$  is sufficiently large, where  $N$  is the cardinality of the point set  $P$ ,  $P$  is a quadrature rule in  $[0, 1]^s$ , and  $C'_G$  and  $C_G$  are constants depending only on the cardinality of  $G$ . These bounds generalize the bounds given by Yoshiki and others given for  $G = \mathbb{F}_2$ .

*Keywords:* Quasi-Monte Carlo, numerical integration, WAFOM, digital nets, mean square error,

## 1 Introduction

For an integrable function  $f: [0, 1]^s \rightarrow \mathbb{R}$  and a finite point set in an  $s$ -dimensional unit cube  $\mathcal{P} \subset [0, 1]^s$ , quasi Monte-Carlo (QMC) integration of  $f$  by  $\mathcal{P}$  is an

---

\*The work of the first author was supported by the Program for Leading Graduate Schools, MEXT, Japan.

<sup>†</sup>Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo 153-8914 Japan (ksuzuki@ms.u-tokyo.ac.jp).

approximation value

$$I_{\mathcal{P}}(f) := \frac{1}{N} \sum_{\mathbf{x} \in \mathcal{P}} f(\mathbf{x})$$

of the actual integration

$$I(f) := \int_{[0,1]^s} f(\mathbf{x}) d\mathbf{x},$$

where  $N := |\mathcal{P}|$  is the cardinality of  $\mathcal{P}$ . Thus the QMC integration error is  $\text{Err}(f; \mathcal{P}) := |I_{\mathcal{P}}(f) - I(f)|$ . If the integrand  $f$  has bounded variation in the sense of Hardy and Krause, the Koksma-Hlawka inequality shows that  $\text{Err}(f; \mathcal{P}) \leq V(f)D(\mathcal{P})$ , where  $V(f)$  is the total variation of  $f$  and  $D(\mathcal{P})$  is the star discrepancy of  $\mathcal{P}$ . There are many studies on the construction of point sets with small  $D(\mathcal{P})$ . In particular, digital nets and sequences are a general framework for the construction of good point sets. We refer to [4] and [10] for the general information on QMC integration and digital nets and sequences.

Dick gave quadrature rules for  $\alpha$ -smooth integrands which achieve the optimal rate of convergence [1]. He introduced the Walsh figure of merit (WAFOM)  $\text{WF}_{\alpha}(\mathcal{P})$  (he did not give a name and we use the name in [8]) for a digital net  $\mathcal{P}$  over a finite field with cardinality  $b$ , and proved a Koksma-Hlawka type inequality, namely he proved that  $\text{Err}(f; \mathcal{P}) \leq C_{b,s,\alpha} \|f\|_{\alpha} \cdot \text{WF}_{\alpha}(\mathcal{P})$  holds for any  $\alpha$ -smooth function  $f$ , where  $\|f\|_{\alpha}$  is a norm of  $f$  for a Sobolev space and  $C_{b,s,\alpha}$  is a constant depend only on  $b$ ,  $s$ , and  $\alpha$ . Moreover, he constructed sequences whose  $\text{WF}_{\alpha}$  is of order  $O(N^{-\alpha}(\log N)^{s\alpha})$ . Later he improve the constant factor of the lowest  $\text{WF}_{\alpha}$  for digital nets over a finite cyclic group [2].

On the other hand, to compute  $\text{WF}_{\alpha}$  for a given  $\mathcal{P}$  seems not easy for general  $\alpha$ , so  $\text{WF}_{\alpha}$  seems difficult to use in searching for a good point set by a random search. As a practically computable measure of goodness of a QMC point set from a digital net, Matsumoto, Saito, and Matoba introduced the Walsh figure of merit (WAFOM)  $\text{WF}(P)$  for an  $\mathbb{F}_2$ -digital net  $P$  [8]. They consider an  $\mathbb{F}_2$ -digital net  $P$  as a linear subspace of  $\mathbb{F}_2^{s \times n}$  and define the Dick weight  $\mu: \mathbb{F}_2^{s \times n} \rightarrow \mathbb{Z}$  as

$$\mu((a_{i,j})_{1 \leq i \leq s, 1 \leq j \leq n}) := \sum_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} j \times a_{i,j},$$

where each  $a_{i,j} \in \{0, 1\}$  is considered as an integer, not as an element of  $\mathbb{F}_2$ . Then for an  $\mathbb{F}_2$ -digital net  $P$ , WAFOM is defined as

$$\text{WF}(P) := \sum_{A \in P^{\perp} \setminus \{O\}} 2^{-\mu(A)}.$$

WAFOM is a discretized version of Dick's method in the dyadic case, and thus also satisfies a Koksma-Hlawka type inequality (with some errors due to discretization). Moreover, they showed an inversion formula which computes WAFOM in only  $O(nsN)$  steps. Their numerical experiments showed that a random search of low-WAFOM point sets works well. Later, Matsumoto

and Yoshiaki proved the existence of low-WAFOM point sets [9], and Suzuki proved that the interlacing construction for higher order QMC point sets with Niederreiter-Xing sequences over a finite field gives low-WAFOM point sets [13].

In this paper, as a generalization of [8] we propose the Dick weight and WAFOM for digital nets over a general finite abelian group  $G$ . WAFOM we propose is also a discretized version of Dick's method, but we consider a general  $b$ -adic cases. WAFOM we propose also satisfies a Koksma-Hlawka type inequality if  $G$  is cyclic, and thus is also a measure of goodness of a QMC point set from a digital net. Moreover, we give the MacWilliams identity of weight enumerator polynomials for the Dick weight, with which we can obtain a computable formula of WAFOM. This formula is a generalization of the dyadic case. In addition, we give generalizations of known properties of WAFOM over  $\mathbb{F}_2$  in [9] and [14]. More precisely, we give a lower bound on WAFOM and prove the existence of low-WAFOM point sets. In particular, we modify and improve on some of the results in [9]. These results imply that there exist positive constants  $C, D, D'$  and  $F$  depending only on  $b$  and independent of  $s, n$  and  $N$  such that  $N^{-C \log N/s} \leq \min\{\text{WF}(P) \mid P \text{ is a digital net, } |P| \leq N\} \leq FN^{-D(\log N)/s+D'}$ , if  $(\log N)/s$  is sufficiently large.

These results are similar to the works of Dick, but there is no implication between them. Dick fixed the smoothness  $\alpha$ , while our method requires  $n$ -smoothness on the function where  $n$  is as above. Thus, in our case, the function class is getting smaller for  $n$  being increased.

The rest of the paper is organized as follows. In Section 2, we introduce the necessary background and notation, such as the discretization scheme of QMC integration, the discrete Fourier transformation, and Walsh functions. In Section 3, we define the Dick weight and WAFOM over a general finite abelian group  $G$ , and prove a Koksma-Hlawka type inequality in the case that  $G$  is cyclic. In Section 4, we define the weight enumerator polynomial, and give a computable formula of WAFOM. In Section 5, we consider the case that the precision  $n$  goes to infinity. In Section 6, we give a lower bound on WAFOM, prove the existence of low-WAFOM point sets, and study the order of WAFOM.

## 2 Preliminaries

Throughout this paper, we use the following notation. Let  $\mathbb{N}$  be the set of positive integers and  $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ . Let  $b$  be an integer greater than 1. Let  $\mathbb{Z}_b = \mathbb{Z}/b\mathbb{Z}$  be the residue class ring modulo  $b$ . We identify  $\mathbb{Z}_b$  with the set  $\{0, 1, \dots, b-1\} \subset \mathbb{Z}$ . For a set  $S$ , we denote by  $|S|$  the cardinality of  $S$ . For a group or a ring  $R$  and positive integers  $s$  and  $n$ , we denote by  $R^{s \times n}$  the set of  $s \times n$  matrices with components in  $R$ . We denote by  $O$  the zero matrix. We denote by  $e$  the base of the natural logarithm.

## 2.1 Discretized QMC in base $b$

In this subsection, we explain quasi-Monte Carlo (QMC) and discretized QMC in base  $b$  (see [4] and [10] about QMC for details). This discretization is a straight forward generalization of the  $b = 2$  case in [8].

Let  $s, n$  be positive integers. Let  $\mathcal{P} \subset [0, 1)^s$  be a point set in an  $s$ -dimensional unit cube with finite cardinality  $|\mathcal{P}| = N$ , and let  $f: [0, 1)^s \rightarrow \mathbb{R}$  be an integrable function. Recall that quasi-Monte Carlo integration by  $\mathcal{P}$  is an approximation value

$$I_{\mathcal{P}}(f) := \frac{1}{N} \sum_{\mathbf{x} \in \mathcal{P}} f(\mathbf{x})$$

of the actual integration

$$I(f) := \int_{[0, 1)^s} f(\mathbf{x}) d\mathbf{x}.$$

The QMC integration error is  $\text{Err}(f; \mathcal{P}) := |I_{\mathcal{P}}(f) - I(f)|$ .

Here, we fix a positive integer  $n$ , which is called the degree of discretization or the precision. We consider an  $n$ -digit discrete approximation in base  $b$ .

We associate a matrix  $B := (b_{i,j}) \in \mathbb{Z}_b^{s \times n}$  with a point  $\mathbf{x}_B = (x_B^1, \dots, x_B^s) = (\sum_{j=1}^n b_{1,j} b^{-j}, \dots, \sum_{j=1}^n b_{s,j} b^{-j}) \in [0, 1)^s$ , and with an  $s$ -dimensional cube  $\mathbf{I}_B := \prod_{i=1}^s I_{b_i} \subset [0, 1)^s$ , where each edge  $I_{b_i} := [x_B^i, x_B^i + b^{-n})$  is a half-open interval with length  $b^{-n}$ . We define  $n$ -digit discrete approximation  $f_n$  of  $f$  as

$$f_n: \mathbb{Z}_b^{s \times n} \rightarrow \mathbb{R}, \quad B := (b_{i,j}) \mapsto \frac{1}{\text{Vol}(\mathbf{I}_B)} \int_{\mathbf{I}_B} f(\mathbf{x}) d\mathbf{x}.$$

Let  $P$  be a subset of  $\mathbb{Z}_b^{s \times n}$ . We define  $n$ -th discretized QMC integration of  $f$  by  $P$  as

$$I_{P,n}(f) := \frac{1}{|P|} \sum_{B \in P} f_n(B)$$

and define the  $n$ -th discretized QMC integration error as

$$\text{Err}(f; P, n) := |I_{P,n}(f) - I(f)|.$$

For each  $B \in P$ , we take the center point of the cube  $\mathbf{I}_B$ . Let  $\mathcal{P} \subset [0, 1)^s$  be the set of such center points given by  $P$ . By a slight extension of [8, Lemma 2.1], if  $f$  is continuous with Lipschitz constant  $K$  then we have  $|I_{P,n}(f) - I_{\mathcal{P}}(f)| \leq K\sqrt{s}b^{-n}$ . We take  $n$  large enough so that  $K\sqrt{s}b^{-n}$  is negligibly small compared to the order of QMC integration error  $|I_{\mathcal{P}}(f) - I(f)|$  by  $\mathcal{P}$ . Then we may regard the  $n$ -th discretized QMC integration error  $\text{Err}(f; P, n)$  as an approximation of the QMC integration error  $\text{Err}(f; P)$ .

As point sets, in this paper we consider subgroups of  $\mathbb{Z}_b^{s \times n}$  as well as digital nets. Digital nets are point sets in  $[0, 1)^s$  whose construction is based on linear algebra over a finite field (or more generally finite rings). The definition of digital nets over a finite ring is given in [5]. we adopt an equivalent definition of digital nets, which is proposed as digital nets with generating matrices in [3, Definition 4.3].

**Definition 2.1.** Let  $C_1, \dots, C_s \in \mathbb{Z}_b^{n \times d}$  be matrices and let  $X_1, \dots, X_d \in \mathbb{Z}_b^{s \times n}$  be defined by the  $j$ -th row of  $X_i$  is the transpose of the  $i$ -th column of  $C_j$ . Assume that  $X_1, \dots, X_d$  are a free basis of  $\mathbb{Z}_b^{s \times n}$  as a  $\mathbb{Z}_b$ -module. For an integer  $k$  with  $0 \leq k \leq b^d - 1$ , we define a matrix  $\mathbf{x}_k \in \mathbb{Z}_b^{s \times n}$  as  $\mathbf{x}_k = \sum_{i=1}^d \kappa_{i-1} X_i$ , where  $k = \kappa_0 + \kappa_1 b^1 + \dots + \kappa_{d-1} b^{d-1}$  ( $0 \leq \kappa_i \leq b-1$ ) is the  $b$ -adic expansion of  $k$ . We call the set  $\{\mathbf{x}_0, \dots, \mathbf{x}_{b^d-1}\}$  the digital net generated by the matrices  $C_1, \dots, C_s$ .

It is easy to see that digital nets become subgroups of  $\mathbb{Z}_b^{s \times n}$ .

## 2.2 Discrete Fourier transformation

In this subsection, we recall the notion of character groups and the discrete Fourier transformation. We refer to [12] for general information on character groups. Let  $G$  be a finite abelian group. Let  $T := \{z \in \mathbb{C} \mid |z| = 1\}$  be the multiplicative group of complex numbers of absolute value one. Let  $\omega_b = \exp(2\pi\sqrt{-1}/b)$ .

**Definition 2.2.** We define the character group of  $G$  by  $G^\vee := \text{Hom}(G, T)$ , namely  $G^\vee$  is the set of group homomorphisms from  $G$  to  $T$ .

There is a natural pairing  $\bullet: G^\vee \times G \rightarrow T$ ,  $(h, g) \mapsto h \bullet g := h(g)$ .

We can see that  $\mathbb{Z}_b^\vee$  is isomorphic to  $\mathbb{Z}_b$  as an abstract group. Throughout this paper, we identify  $\mathbb{Z}_b^\vee$  with  $\mathbb{Z}_b$  through a pairing  $\bullet: \mathbb{Z}_b \times \mathbb{Z}_b \rightarrow T$ ,  $(h, g) \mapsto h \bullet g := \omega_b^{hg}$ , where  $hg$  is the product in  $\mathbb{Z}_b$ .

Let  $R$  be a commutative ring containing  $\mathbb{C}$ . Let  $f: G \rightarrow R$  be a function. We define the discrete Fourier transformation of  $f$  as below.

**Definition 2.3.** The discrete Fourier transformation of  $f$  is defined by  $\hat{f}: G^\vee \rightarrow R$ ,  $h \mapsto \frac{1}{|G|} \sum_{g \in G} f(g)(h \bullet g)$ . Each value  $\hat{f}(h)$  is called a discrete Fourier coefficient.

We assume that  $P \subset G$  is a subgroup. We define  $P^\perp := \{h \in G^\vee \mid h \bullet g = 1 \text{ for all } g \in P\}$ . Since  $P^\perp$  is the kernel of the surjection map  $G^\vee \rightarrow P^\vee$ , we have  $|P^\perp| = |G|/|P|$ . We recall the orthogonality of characters.

**Lemma 2.4.** Suppose that  $P \subset G$  is a subgroup and  $g \in G$ . Then we have

$$\sum_{h \in P^\perp} h \bullet g = \begin{cases} |P^\perp| & \text{if } g \in P, \\ 0 & \text{if } g \notin P. \end{cases}$$

This lemma implies the Poisson summation formula and the Fourier inversion formula.

**Theorem 2.5** (Poisson summation formula).

$$\frac{1}{|P|} \sum_{g \in P} f(g) = \sum_{h \in P^\perp} \hat{f}(h).$$

*Proof.*

$$\begin{aligned}
\sum_{h \in P^\perp} \widehat{f}(h) &= \sum_{h \in P^\perp} \frac{1}{|G|} \sum_{g \in G} (h \bullet g) f(g) \\
&= \sum_{g \in G} \frac{1}{|G|} f(g) \sum_{h \in P^\perp} h \bullet g \\
&= \frac{1}{|G|} \sum_{g \in P} f(g) \cdot |P^\perp| \quad (\because \text{Lemma 2.4}) \\
&= \frac{1}{|P|} \sum_{g \in P} f(g). \quad \square
\end{aligned}$$

**Theorem 2.6** (Fourier inversion formula). *For a complex-valued function  $f: G \rightarrow \mathbb{C}$ , we have  $f(g) = \sum_{h \in G^\vee} \widehat{f}(-h)(h \bullet g)$  for any  $g \in G$ . Moreover, if  $f$  is real-valued, we have  $f(g) = \sum_{h \in G^\vee} \widehat{f}(h)(h \bullet g)$ .*

*Proof.* By Lemma 2.4, we have  $\sum_{h \in G^\vee} h \bullet g = 0$  if  $g \neq 0$  and  $\sum_{h \in G^\vee} h \bullet g = |G|$  if  $g = 0$ . Thus we have

$$\begin{aligned}
\sum_{h \in G^\vee} \widehat{f}(-h)(h \bullet g) &= \sum_{h \in G^\vee} \frac{1}{|G|} \sum_{g' \in G} f(g')((-h) \bullet g')(h \bullet g) \\
&= \frac{1}{|G|} \sum_{h \in G^\vee} f(g') \sum_{g' \in G} (h \bullet (g - g')) \\
&= f(g),
\end{aligned}$$

which proves the complex-valued case. If  $f$  is real-valued, we have  $\widehat{f}(-h) = \overline{\widehat{f}(h)}$ , and thus the complex-valued case implies the real-valued case.  $\square$

## 2.3 Walsh functions

In this subsection, we recall the notion of Walsh functions and Walsh coefficients, and see the relationship between Walsh coefficients and discrete Fourier coefficients. As a corollary, we prove that considering  $n$ -digit discrete approximation  $f_n$  of  $f$  is as same as considering the appropriate approximation of the Walsh series of  $f$ . We refer to [4, Appendix A] for general information on Walsh functions.

First, we define Walsh functions for the one dimensional case.

**Definition 2.7.** *Let  $k \in \mathbb{N}_0$  with  $b$ -adic expansion  $k = \kappa_0 + \kappa_1 b^1 + \kappa_2 b^2 + \dots$  (this expansion is actually finite), where  $\kappa_j \in \{0, 1, \dots, b-1\}$  for all  $j \in \mathbb{N}_0$ . The  $k$ -th  $b$ -adic Walsh function  ${}_b\text{wal}_k: [0, 1) \rightarrow \{0, \omega_b, \dots, \omega_b^{b-1}\}$  is defined as*

$${}_b\text{wal}_k := \omega_b^{\kappa_0 x_1 + \kappa_1 x_2 + \dots},$$

for  $x \in [0, 1)$  with  $b$ -adic expansion  $x = x_1 b^{-1} + x_2 b^{-2} + x_3 b^{-3} + \dots$  with  $x_j \in \{0, 1, \dots, b-1\}$ , which is unique in the sense that infinitely many of the  $x_j$  must be different from  $b-1$ .

This definition is generalized to higher-dimensional case.

**Definition 2.8.** For dimension  $s \geq 1$ , let  $\mathbf{x} = (x_1, \dots, x_s) \in [0, 1]^s$  and let  $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ . The  $\mathbf{k}$ -th  $b$ -adic Walsh function  ${}_b\text{wal}_{\mathbf{k}}: [0, 1]^s \rightarrow \{0, \omega_b, \dots, \omega_b^{b-1}\}$  is defined as

$${}_b\text{wal}_{\mathbf{k}}(\mathbf{x}) = \prod_{i=1}^s {}_b\text{wal}_{k_i}(x_i).$$

Walsh coefficients are defined as follows.

**Definition 2.9.** Let  $f: [0, 1]^s \rightarrow \mathbb{R}$ . The  $\mathbf{k}$ -th  $b$ -adic Walsh coefficient of  $f$  is defined as

$$\mathcal{F}(f)(\mathbf{k}) := \int_{[0, 1]^s} f(\mathbf{x}) \overline{{}_b\text{wal}_{\mathbf{k}}(\mathbf{x})} d\mathbf{x}.$$

We see the relationship between Walsh coefficients and discrete Fourier coefficients in the following. Let  $A = (a_{i,j}) \in \mathbb{Z}_b^{s \times n}$ . We define maps  $\phi_i: \mathbb{Z}_b^{s \times n} \rightarrow \mathbb{N}_0$  as  $\phi_i(A) = \sum_{j=1}^n a_{i,j} b^{j-1}$  and  $\phi: \mathbb{Z}_b^{s \times n} \rightarrow \mathbb{N}_0^s$  as  $\phi(A) = (\phi_1(A), \dots, \phi_s(A))$ . Note that  $\phi_i(A) < b^n$  follows for all  $1 \leq i \leq s$  and  $A \in \mathbb{Z}_b^{s \times n}$ .

**Lemma 2.10.** Let  $f: [0, 1]^s \rightarrow \mathbb{R}$  and  $A = (a_{i,j}) \in \mathbb{Z}_b^{s \times n}$ . Then we have

$$\overline{\mathcal{F}(f)(\phi(A))} = \widehat{f_n}(A).$$

*Proof.* Since  $\phi_i(A) < b^n$  holds for all  $1 \leq i \leq s$ , for all  $\mathbf{x} = (x_1, \dots, x_s) \in \mathbf{I}_B$  we have

$${}_b\text{wal}_{\phi(A)}(\mathbf{x}) = \prod_{i=1}^s {}_b\text{wal}_{\phi_i(A)}(x_i) = \prod_{i=1}^s \omega_b^{a_{i,1}b_{i,1} + \dots + a_{i,n}b_{i,n}} = B \bullet A.$$

Therefore we have

$$\begin{aligned} \overline{\mathcal{F}(f)(\phi(A))} &= \int_{[0, 1]^s} f(\mathbf{x}) {}_b\text{wal}_{\phi(A)}(\mathbf{x}) d\mathbf{x} = \sum_{B \in \mathbb{Z}_b^{s \times n}} \int_{\mathbf{I}_B} f(\mathbf{x}) {}_b\text{wal}_{\phi(A)}(\mathbf{x}) d\mathbf{x} \\ &= \sum_{B \in \mathbb{Z}_b^{s \times n}} \int_{\mathbf{I}_B} f(\mathbf{x}) (B \bullet A) d\mathbf{x} \\ &= \sum_{B \in \mathbb{Z}_b^{s \times n}} (B \bullet A) \int_{\mathbf{I}_B} f(\mathbf{x}) d\mathbf{x} \\ &= \sum_{B \in \mathbb{Z}_b^{s \times n}} (B \bullet A) \cdot \text{Vol}(\mathbf{I}_B) f_n(B) \\ &= \sum_{B \in \mathbb{Z}_b^{s \times n}} (B \bullet A) \cdot b^{-sn} f_n(B) \\ &= \widehat{f_n}(A), \end{aligned}$$

which proves the lemma.  $\square$

Let  $f \sim \sum_{\mathbf{k} \in \mathbb{N}_0^s} \mathcal{F}(f)(\mathbf{k})_b \text{wal}_{\mathbf{k}}$  be the Walsh expansion of a real valued function  $f: [0, 1]^s \rightarrow \mathbb{R}$ . Lemma 2.10 implies that considering  $n$ -digit discrete approximation  $f_n$  of  $f$  is as same as considering the Walsh polynomial  $\sum_{\mathbf{k} < b^n} \mathcal{F}(f)(\mathbf{k})_b \text{wal}_{\mathbf{k}}$ , where  $\mathbf{k} = (k_1, \dots, k_s) < b^n$  means that  $k_i < b^n$  holds for every  $i = 1, \dots, s$ , namely we have the following.

**Proposition 2.11.** *Let  $f: [0, 1]^s \rightarrow \mathbb{R}$ . For  $B \in \mathbb{Z}_b^{s \times n}$ , we have  $f_n(B) = \sum_{\mathbf{k} < b^n} \mathcal{F}(f)(\mathbf{k})_b \text{wal}_{\mathbf{k}}(\mathbf{x}_B)$ .*

*Proof.*

$$\begin{aligned} f_n(B) &= \sum_{A \in \mathbb{Z}_b^{s \times n}} \overline{\widehat{f_n(A)B} \bullet A} \quad (\because \text{Lemma 2.6}) \\ &= \sum_{A \in \mathbb{Z}_b^{s \times n}} \mathcal{F}(f)(\phi(A))_b \text{wal}_{\phi(A)}(\mathbf{x}_B) \quad (\because \text{Lemma 2.10}) \\ &= \sum_{\mathbf{k} < b^n} \mathcal{F}(f)(\mathbf{k})_b \text{wal}_{\mathbf{k}}(\mathbf{x}_B). \end{aligned} \quad \square$$

### 3 WAFOM for digital nets over a finite abelian group

In this section, we expand the notion of WAFOM defined in [8], more precisely, we define WAFOM over a finite abelian group with  $b$  elements.

First, we evaluate the  $n$ -th discretized QMC integration error of  $f$  with its discrete Fourier coefficients. Let  $P \subset \mathbb{Z}_b^{s \times n}$  be a subgroup. We have  $I(f) = \widehat{f_n}(O)$  by the definition of the discrete Fourier inversion, and we have  $I_{P,n}(f) = \sum_{A \in P^\perp} \widehat{f_n}(A)$  by the Poisson summation formula (Theorem 2.5). Hence we have

$$\text{Err}(f; P, n) = |I_{P,n}(f) - I(f)| = \left| \sum_{A \in P^\perp \setminus \{O\}} \widehat{f_n}(A) \right| \leq \sum_{A \in P^\perp \setminus \{O\}} |\widehat{f_n}(A)|,$$

and thus we would like to bound the value  $|\widehat{f_n}(A)|$ . Dick gives an upper bound of the  $\mathbf{k}$ -th  $b$ -adic Walsh coefficient  $\mathcal{F}(f)(\mathbf{k})$  for  $n$ -smooth function  $f$  (for the definition of  $n$ -smoothness, see [1] or [4, §14]).

**Theorem 3.1** ([4], Theorem 14.23). *There is a constant  $C_{b,s,n}$  depending only on  $b, s$  and  $n$  such that for any  $n$ -smooth function  $f: [0, 1]^s \rightarrow \mathbb{R}$  and any  $\mathbf{k} \in \mathbb{N}^s$  it holds that*

$$|\mathcal{F}(f)(\mathbf{k})| \leq C_{b,s,n} \|f\|_n \cdot b^{-\mu_n(\mathbf{k})},$$

where  $\|f\|_n$  is a norm of  $f$  for a Sobolev space and  $\mu_n(\mathbf{k})$  is the  $n$ -weight of  $\mathbf{k}$ , which are defined in [4, (14.6) and Theorem 14.23] (we do not define them here).



Instead of  $\mu_n$ , we define the Dick weight  $\mu$  on dual groups of general finite abelian groups below, which is a generalization of the Dick weight over  $\mathbb{F}_2$  defined in [8]. Actually,  $\mu$  is a special case of  $\mu_n \circ \phi$ . More precisely, if  $G = \mathbb{Z}_b$  and  $\alpha \geq n$  hold, then we have  $\mu = \mu_\alpha \circ \phi$  as a function from  $(\mathbb{Z}_b^\vee)^{s \times n} (\simeq \mathbb{Z}_b^{s \times n})$  to  $\mathbb{N}_0$ .

**Definition 3.2.** Let  $G$  be a finite abelian group and let  $A \in (G^\vee)^{s \times n}$ . The Dick weight  $\mu: (G^\vee)^{s \times n} \rightarrow \mathbb{N}_0$  is defined as

$$\mu(A) := \sum_{i,j} j \times \delta(a_{i,j}),$$

with  $\delta(h) = 0$  for  $h = 0$  and  $\delta(h) = 1$  for  $h \neq 0$ .

We obtain the next corollary.

**Corollary 3.3.** There exists a constant  $C_{b,s,n}$  depending only on  $b, s$  and  $n$  such that for any  $n$ -smooth function  $f: [0, 1]^s \rightarrow \mathbb{R}$  and any  $A \in (\mathbb{Z}_b)^{s \times n}$  it holds that

$$|\widehat{f_n}(A)| \leq C_{b,s,n} \|f\|_n \cdot b^{-\mu(A)}.$$

*Proof.* This is the direct corollary of Theorem 3.1, Lemma 2.10, and the equality  $\mu(A) = \mu_n \circ \phi(A)$ .  $\square$

By the above corollary, we have a bound on the  $n$ -th discretized QMC integration error

$$\text{Err}(f; P, n) := |I(f) - I_{P,n}(f)| \leq C_{b,s,n} \|f\|_n \times \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)},$$

for a subgroup  $P$  of  $\mathbb{Z}_b^{s \times n}$ .

Hence, as a generalization of [8], we define a kind of figure of merit (Walsh figure of merit or WAFOM).

**Definition 3.4.** Let  $s, n$  be positive integers. Let  $G$  be a finite abelian group with  $b$  elements. Let  $P \subset G^{s \times n}$  be a subgroup of  $G^{s \times n}$ . We define Walsh figure of merit of  $P$  by

$$\text{WF}(P) := \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)}.$$

In order to stress the role of the precision  $n$ , we sometimes denote  $\text{WF}^n(P)$  instead of  $\text{WF}(P)$ .

Then, as we have seen, we have the Koksma-Hlawka type inequality

$$\text{Err}(f; P, n) := |I(f) - I_{P,n}(f)| \leq C_{b,s,n} \|f\|_n \times \text{WF}(P)$$

for a subgroup  $P \subset \mathbb{Z}_b^{s \times n}$ . This shows that  $\text{WF}(P)$  is a quality measure of the point set  $P$  for quasi-Monte Carlo integration when  $G = \mathbb{Z}_b$ .

## 4 MacWilliams identity over an abelian group

In this section, we assume that  $s, n$  are positive integers. Recall that  $G$  is a finite abelian group and  $G^\vee$  its character group. We consider an abelian group  $G^{s \times n}$ . Let  $P \subset G^{s \times n}$  be a subgroup.

We are interested in the weight enumerator polynomial of  $P^\perp$

$$W_{P^\perp}(x, y) := \sum_{A \in P^\perp} x^{M - \mu(A)} y^{\mu(A)} \in \mathbb{C}[x, y],$$

where  $M := n(n+1)s/2$ .

Let  $R := \mathbb{C}[x_{i,j}(h)]$ , where  $x_{i,j}(h)$  is a family of indeterminates for  $1 \leq i \leq s$ ,  $1 \leq j \leq n$ , and  $h \in G^\vee$ . We define functions  $f_{i,j}: G^\vee \rightarrow R$  as  $f_{i,j}(h) = x_{i,j}(h)$  and  $f: (G^{s \times n})^\vee = (G^\vee)^{s \times n} \rightarrow R$  as

$$f(A) := \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} f_{i,j}(a_{i,j}) = \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} x_{i,j}(a_{i,j}).$$

Now the complete weight enumerator polynomial of  $P^\perp$ , in a standard sense [6, Chapter 5], is defined by

$$GW_{P^\perp}(x_{i,j}(h)) := \sum_{A \in P^\perp} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} x_{i,j}(a_{i,j}),$$

and similarly, the complete weight enumerator polynomial of  $P$  is defined by

$$GW_P^*(x_{*i,j}(g)) := \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} x_{*i,j}(b_{i,j})$$

in  $R^* := \mathbb{C}[x_{*i,j}(g)]$  where  $x_{*i,j}(g)$  is a family of indeterminates for  $1 \leq i \leq s$ ,  $1 \leq j \leq n$ , and  $g \in G$ . We note that if we substitute

$$x_{i,j}(0) \leftarrow x^j, \quad x_{i,j}(h) \leftarrow y^j \text{ for } h \neq 0, \quad (1)$$

we have an identity

$$GW_{P^\perp}(x_{i,j}(h))|_{\text{above substitution}} = W_{P^\perp}(x, y).$$

A standard formula of the Fourier transformation tells that, if  $f_1: G_1 \rightarrow R$ ,  $f_2: G_2 \rightarrow R$  are functions and  $f_1 f_2: G_1 \times G_2 \rightarrow R$  is their multiplication at the value, then

$$\widehat{f_1 f_2} = \widehat{f_1} \widehat{f_2}$$

holds. This implies that

$$\widehat{f}(B) = \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} \widehat{f_{i,j}}(b_{i,j}) = \frac{1}{|G|^{sn}} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} \sum_{h \in G^\vee} f_{i,j}(h)(h \bullet b_{i,j}).$$

Hence, by the Poisson summation formula (Theorem 2.5), we have

$$\begin{aligned}
GW_{P^\perp}(x_{i,j}(h)) &= \sum_{A \in P^\perp} f(A) \\
&= |P^\perp| \sum_{B \in P} \hat{f}(B) \\
&= \frac{1}{|P|} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} \sum_{h \in G^\vee} f_{i,j}(h)(h \bullet b_{i,j}).
\end{aligned}$$

Thus we have the MacWilliams identity below, which is a variant of Generalized MacWilliams identity [6, Chapter 5 §6]:

**Proposition 4.1** (MacWilliams identity).

$$GW_{P^\perp}(x_{i,j}(h)) = \frac{1}{|P|} GW_P^*(substituted),$$

where in the right hand side every  $x_{*i,j}(g)$  is substituted by

$$x_{*i,j}(g) \leftarrow \sum_{h \in G^\vee} (h \bullet g)x_{i,j}(h).$$

We consider specializations of this identity. First, we consider a specialization  $\overline{GW}_{P^\perp}(x_1, \dots, x_n, y_1, \dots, y_n)$  of  $GW_{P^\perp}(x_{i,j}(h))$  obtained by the substitution

$$x_{i,j}(0) \leftarrow x_j, \quad x_{i,j}(h) \leftarrow y_j \text{ for } h \neq 0.$$

We have

$$\begin{aligned}
\sum_{h \in G^\vee} (h \bullet g)x_{i,j}(h) \Big|_{\text{above substitution}} &= (0 \bullet g)x_j + \sum_{h \in G^\vee \setminus \{0\}} (h \bullet g)y_j \\
&= x_j - y_j + \sum_{h \in G^\vee} (h \bullet g)y_j \\
&= x_j - y_j + \begin{cases} by_j & (\text{if } g = 0) \\ 0 & (\text{otherwise}) \end{cases} \\
&= \begin{cases} x_j + (b-1)y_j & (\text{if } g = 0) \\ x_j - y_j & (\text{otherwise}) \end{cases},
\end{aligned}$$

where we use Lemma 2.4 for the third equality. Thus, we have the following formula.

**Corollary 4.2.**

$$\overline{GW}_{P^\perp}(x_1, \dots, x_n, y_1, \dots, y_n) = \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} (x_j + \eta(b_{i,j})y_j),$$

where  $\eta(b_{i,j}) = b-1$  if  $b_{i,j} = 0$  and  $\eta(b_{i,j}) = -1$  if  $b_{i,j} \neq 0$ .

Second, we consider the specialization (1) of  $GW_{P^\perp}$ . We have already seen that  $GW_{P^\perp} \mid_{(\text{substitution (1)})} = W_{P^\perp}(x, y)$  holds. Since

$$W_{P^\perp}(x, y) = \overline{GW}_{P^\perp}(x^1, \dots, x^n, y^1, \dots, y^n)$$

follows, Corollary 4.2 implies the following formula:

**Theorem 4.3.**

$$W_{P^\perp}(x, y) = \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} (x^j + \eta(b_{i,j})y^j),$$

where  $\eta(b_{i,j}) = b - 1$  if  $b_{i,j} = 0$  and  $\eta(b_{i,j}) = -1$  if  $b_{i,j} \neq 0$ .

Using Theorem 4.3, we can compute  $\text{WF}(P)$  and  $\delta_{P^\perp}$ , the minimum Dick weight of  $P^\perp$ . The minimum Dick weight of  $P^\perp$  is defined as  $\delta_{P^\perp} := \min_{B \in P^\perp \setminus \{O\}} \mu(B)$ , which is used for bounding WAFOM (see Section 6.3). First, we introduce how to compute  $\text{WF}(P)$ . The following formula to compute WAFOM is a generalization of [8, Corollary 4.2], which treats the case  $G = \mathbb{F}_2$ .

**Corollary 4.4.** *Let  $P \subset \mathbb{Z}_b^{s \times n}$  be a subgroup. Then we have*

$$\text{WF}(P) = -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} (1 + \eta(b_{i,j})b^{-j}).$$

*Proof.*

$$\begin{aligned} \text{WF}(P) &= \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)} \\ &= -1 + \sum_{A \in P^\perp} b^{-\mu(A)} \\ &= -1 + W_{P^\perp}(1, b^{-1}) \\ &= -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} (1 + \eta(b_{i,j})b^{-j}). \quad \square \end{aligned}$$

The merit of Theorem 4.3 and Corollary 4.4 is that the number of summation depends only on  $|P|$  linearly, not  $|P^\perp| = b^{sn}/|P|$ . We can calculate weight enumerator polynomials by  $sn$  times multiplication between an integer polynomial with a binomial, and  $|P|$  times addition of such polynomials of degree  $n(n+1)/2$ . In the case of computing WAFOM, we need  $sn$  times of multiplication of real numbers and  $|P|$  times of summation of such real numbers, thus we need  $O(sn|P|)$  times of operations of real numbers. On the other hand, to calculate weight enumerator polynomials based on the definition, we need  $|P^\perp|$  times of summations of monomials, and to calculate weight WAFOM based on the definition, we need  $|P^\perp|$  times of summations of real numbers.

For QMC, the size  $|P|$  can not exceed a reasonable number of computer operations, so  $|P^\perp| = b^{sn}/|P|$  can be large if  $sn$  is sufficiently large. This implies that the computational complexity of calculating weight enumerator polynomials or WAFOM using Theorem 4.3 or Corollary 4.4 is smaller if  $sn$  is large.

Second, we introduce how to compute  $\delta_{P^\perp}$ . The minimum Dick weight  $\delta_{P^\perp}$  is equal to the degree of leading nonzero term of  $-1 + W_{P^\perp}(1, y)$ , namely:

**Lemma 4.5.** *Let  $W_{P^\perp}(1, y) = 1 + \sum_{i=1}^{\infty} a_i y^i$ . Then we have  $\delta_{P^\perp} = \min\{i \mid a_i \neq 0\}$ .*

Thus we can obtain the minimum Dick weight of  $P^\perp$  by calculating the weight enumerator polynomial of  $P^\perp$ .

**Remark 4.6.** *Because of Lemma 6.18, in order to compute  $\delta_{P^\perp}$  it is sufficient to compute  $W_{P^\perp}(1, y)$  only up to degree  $\delta_{P^\perp} \leq d^2/(2s) + 3d/2 + s$ .*

## 5 $n \rightarrow \infty$ case

It is natural to consider WAFOM with infinite precision as the  $n \rightarrow \infty$  case. In this case, we consider point sets as a subset of  $G^{s \times \mathbb{N}}$ . We follow the formulation in [8, §5] and [3, §2]. For general properties of character groups, see [3, §2].

The character group  $(G^{s \times \mathbb{N}})^\vee$  of  $G^{s \times \mathbb{N}}$  is isomorphic to  $((G^\vee)^{\oplus \mathbb{N}})^s$ , where  $((G^\vee)^{\oplus \mathbb{N}})^s$  denotes the subset of  $((G^\vee)^{\oplus \mathbb{N}})^s = (G^\vee)^{s \times \mathbb{N}}$  consisting of matrices with all but finite components being zero. The pairing is given by

$$((G^\vee)^{\oplus \mathbb{N}})^s \times G^{s \times \mathbb{N}} \rightarrow T, \quad ((a_{i,j}), (b_{i,j})) \mapsto \prod_{i,j} a_{i,j} \bullet b_{i,j}.$$

Note that all but finitely many of the components of the last product are equal to one.

$(G^\vee)^{s \times n}$  is naturally identified with the subgroup of elements  $((G^\vee)^{\oplus \mathbb{N}})^s$  whose  $m$ -th column is zero for  $m > n$ . Then,  $((G^\vee)^{\oplus \mathbb{N}})^s$  is identified with the union  $\cup_{n=1}^{\infty} (G^\vee)^{s \times n}$ . Thus, any  $A \in ((G^\vee)^{\oplus \mathbb{N}})^s$  is contained in some  $(G^\vee)^{s \times n}$ , and hence  $\mu(A)$  is defined as in Definition 3.4 (it is independent of the choice of  $n$ ).

Let  $P \subset G^{s \times \mathbb{N}}$  a subgroup. We define its orthogonal space  $P^\perp \subset (G^{s \times \mathbb{N}})^\vee$  by

$$P^\perp := \{A \in (G^{s \times \mathbb{N}})^\vee \mid A \bullet B = 1 \ (\forall B \in P)\}.$$

We define infinite precision version of WAFOM by

$$\text{WF}^\infty(P) := \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)}. \quad (2)$$

This infinite sum converges, since by Lemma 6.5 we have

$$\sum_{A \in (G^{s \times \mathbb{N}})^\vee} b^{-\mu(A)} < \sum_{m=0}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} < \infty. \quad (3)$$

Now we consider the relation between  $\text{WF}^n$  and  $\text{WF}^\infty$  in the two cases below.

In the first case, we consider a finite group  $P \subset G^{s \times \infty}$  and the projection from  $(G^{s \times \infty}) \rightarrow G^{s \times n}$  defined as follows. By looking only at the first  $n$  columns, we have a truncation projection

$$\text{pr}_n: (G^{s \times \mathbb{N}}) \rightarrow G^{s \times n}.$$

For a finite subgroup  $P \subset G^{s \times \infty}$ , we may consider its projection  $\text{pr}_n(P) \subset G^{s \times n}$ . We have  $\text{pr}_n(P)^\perp \subset \text{pr}_{n+1}(P)^\perp$  and  $\cup_n \text{pr}_n(P)^\perp = P^\perp$ . Then, using the convergence of (3), it can be seen that

$$\text{WF}^\infty(P) = \lim_{n \rightarrow \infty} \text{WF}^n(\text{pr}_n(P)) \quad (4)$$

for all  $P \subset G^{s \times \infty}$ . Using the convergence of (4), we can see that 4.4 holds when  $n \rightarrow \infty$ , namely

**Proposition 5.1.** *Let  $P \subset G^{s \times \mathbb{N}}$  be a finite subgroup. Then we have*

$$\text{WF}^\infty(P) = -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j < \infty}} (1 + \eta(b_{i,j})b^{-j}).$$

Newly we consider a finite subgroup  $P \subset G^{s \times n}$  as a subset of  $G^{s \times \infty}$  through the injection  $\iota_n: G^{s \times n} \rightarrow G^{s \times \infty}$ , where  $\iota_n$  is given by supplementing 0 column vectors on the right side. We define  $P_\infty := \iota_n(P)$  be a subgroup of  $G^{s \times \infty}$ .

Then for a finite subgroup  $P \subset G^{s \times n}$  we have

$$\begin{aligned} \text{WF}^\infty(P_\infty) &= -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j < \infty}} (1 + \eta(b_{i,j})b^{-j}) \\ &= -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} (1 + \eta(b_{i,j})b^{-j}) \prod_{\substack{1 \leq i \leq s \\ n+1 \leq j < \infty}} (1 + \eta(0)b^{-j}) \\ &\leq -1 + (\text{WF}^n(P) + 1) \exp(sb^{-n}) \\ &= \exp(sb^{-n})\text{WF}^n(P) + \exp(sb^{-n}) - 1, \end{aligned}$$

where we use the following inequality: We have

$$\begin{aligned} \log \left( \prod_{\substack{1 \leq i \leq s \\ n+1 \leq j < \infty}} (1 + \eta(0)b^{-j}) \right) &= s \sum_{j=n+1}^{\infty} \log(1 + (b-1)b^{-j}) \\ &\leq s \sum_{j=n+1}^{\infty} (b-1)b^{-j} \\ &= sb^{-n}, \end{aligned}$$

and thus

$$\prod_{\substack{1 \leq i \leq s \\ n+1 \leq j < \infty}} (1 + \eta(b_{i,j})b^{-j}) \leq \exp(sb^{-n}).$$

On the other hand, we have  $P^\perp \subset (P_\infty)^\perp$  and thus  $\text{WF}^n(P) \leq \text{WF}^\infty(P_\infty)$ .

Now we proved:

**Proposition 5.2.** *Let  $P \subset G^{s \times n}$  be a subgroup. Then we have*

$$\text{WF}^n(P) \leq \text{WF}^\infty(P_\infty) \leq \exp(sb^{-n})\text{WF}^n(P) + \exp(sb^{-n}) - 1.$$

## 6 Estimation of WAFOM

The following arguments from Section 6.1 to Section 6.4, are generalizations of [9] which deals with the case  $G = \mathbb{F}_2$ , and arguments in Section 6.5 are generalizations of [14], which deals with the case  $G = \mathbb{F}_2$ . The methods for proofs are similar to [9] and [14]. In this section, we suppose that  $s$  and  $n$  are positive integers and that  $G$  is a finite abelian group.

### 6.1 Geometry of the Dick weight

Recall that  $G$  is a finite abelian group with  $b \geq 2$  elements,  $G^\vee$  its character group. The Dick weight  $\mu: (G^\vee)^{s \times n} \rightarrow \mathbb{N}_0$  induces a metric

$$d(A, B) := \mu(A - B) \text{ for } A, B \in (G^\vee)^{s \times n}$$

and thus  $(G^\vee)^{s \times n}$  can be regarded as a metric space.

Let  $S_{s,n}(m) := |\{A \in (G^\vee)^{s \times n} \mid \mu(A) = m\}|$ , namely  $S_{s,n}(m)$  is the cardinality of the sphere in  $(G^\vee)^{s \times n}$  with center 0 and radius  $m$ . A combinatorial interpretation of  $S_{s,n}(m)$  is as follows. One has  $s \times n$  dice. Each die has  $b$  faces. For each value  $i = 1, \dots, n$ , there exist exactly  $s$  dice with value 0 on one face and  $i$  on the other  $b - 1$  faces. Then,  $S_{s,n}(m)$  is the number of ways that the summation of the upper surfaces of  $s \times n$  dice is  $m$ . This combinatorial interpretation implies the following identity:

$$\prod_{k=1}^n (1 + (b-1)x^k)^s = \sum_{m=0}^{\infty} S_{s,n}(m)x^m.$$

You can also see this identity from Theorem 4.3 for  $P = \{O\}$ ,  $x \leftarrow 1$ , and  $y \leftarrow x$ . Note that the right hand side is a finite sum. It is easy to see that  $S_{s,n}(m)$  is monotonically increasing with respect to  $s$  and  $n$ , and  $S_{s,m}(m) = S_{s,m+1}(m) = S_{s,m+2}(m) = \dots$  holds.

**Definition 6.1.**  $S_s(m) := S_{s,m}(m)$ .

We have the following identity between formal power series:

$$\prod_{k=1}^{\infty} (1 + (b-1)x^k)^s = \sum_{m=0}^{\infty} S_s(m)x^m. \quad (5)$$

For any positive integer  $M$ , we define

$$\mathcal{B}_{s,n}(M) := \{A \in (G^{\vee})^{s \times n} \mid \mu(A) \leq M\}, \quad \text{vol}_{s,n}(M) := |\mathcal{B}_{s,n}(M)|,$$

namely  $\mathcal{B}_{s,n}(M)$  is the ball in  $G^{s \times n}$  with center 0 and radius  $M$ , and  $\text{vol}_{s,n}(M)$  is its cardinality. We have  $\text{vol}_{s,n}(M) = \sum_{m=0}^M S_{s,n}(m)$ , and thus  $\text{vol}_{s,n}(M)$  inherits properties of  $S_{s,n}(m)$ , namely,  $\text{vol}_{s,n}(M)$  is also monotonically increasing with respect to  $s$  and  $n$ , and  $\text{vol}_{s,M}(M) = \text{vol}_{s,M+1}(M) = \text{vol}_{s,M+2}(M) = \dots$  holds.

**Definition 6.2.**  $\text{vol}_s(M) := \text{vol}_{s,M}(M)$ .

**Remark 6.3.** The above consideration can be applied to the case of  $n = \infty$ . Namely, we define

$$\begin{aligned} S_{s,\infty}(m) &:= |\{A \in (G^{s \times \infty})^{\vee} \mid \mu(A) = m\}|, \\ \mathcal{B}_{s,\infty}(M) &:= \{A \in (G^{s \times \infty})^{\vee} \mid \mu(A) \leq M\}, \\ \text{vol}_{s,\infty}(M) &:= |\mathcal{B}_{s,\infty}(M)|, \end{aligned}$$

and then we have the following identity between formal power series:

$$\prod_{k=1}^{\infty} (1 + (b-1)x^k)^s = \sum_{m=0}^{\infty} S_{s,\infty}(m)x^m.$$

We note that  $S_s(m) = S_{s,\infty}(m)$  and  $\text{vol}_s(M) = \text{vol}_{s,\infty}(M)$  hold.

## 6.2 Combinatorial inequalities

**Lemma 6.4.**

$$\text{vol}_{s,n}(M) \leq \text{vol}_s(M) \leq \exp(2\sqrt{(b-1)sM}).$$

*Proof.* We have already seen the first inequality. We prove the next inequality along [7, Exercise 3(b), p.332], which treats only  $S = 1$  and  $b = 2$  case. If  $M = 0$  it is trivial, and so we assume that  $M > 0$ . Define a polynomial with non-negative integer coefficients by

$$f_{s,M}(x) := \prod_{k=1}^M (1 + (b-1)x^k)^s.$$

Since  $f_{s,M}(x)$  has only non-negative coefficients, from Identity (5) we have  $\sum_{m=0}^M S_s(m)x^m \leq f_{s,M}(x)$  ( $x \in (0, 1)$ ). Hence we have

$$\text{vol}_s(M) = \sum_{m=0}^M S_s(m) \leq \sum_{m=0}^M S_s(M)x^{m-M} \leq f_{s,M}(x)/x^M \quad (x \in (0, 1)).$$



By taking the logarithm of the both sides and using the well-known inequality  $\log(1 + X) \leq X$ , for all  $x \in (0, 1)$  we have

$$\begin{aligned} \text{vol}_{s,n}(M) &\leq s \sum_{k=1}^M \log(1 + (b-1)x^k) + M \log(1/x) \\ &< s(b-1) \sum_{k=1}^M x^k + M \log\left(1 + \frac{1-x}{x}\right) \\ &< s(b-1) \frac{x}{1-x} + M \frac{1-x}{x}. \end{aligned}$$

By comparison of the arithmetic mean and the geometric mean, the last expression attains the minimum value  $2\sqrt{(b-1)sM}$  when  $s(b-1)x/(1-x) = M(1-x)/x$  holds, namely  $x = (1 + \sqrt{(b-1)s/M})^{-1} \in (0, 1)$ .  $\square$

**Lemma 6.5.**

$$S_{s,n}(M) \leq S_s(M) \leq \exp(2\sqrt{(b-1)sM}).$$

*Proof.* It follows from Lemma 6.4 and the inequality  $S_s(M) \leq \text{vol}_s(M)$ .  $\square$

### 6.3 Bounding WAFOM by the minimum weight

**Definition 6.6.** Let  $P \subset G^{s \times n}$  be a subgroup. The minimum Dick weight of  $P^\perp$  is defined by

$$\delta_{P^\perp} := \min_{B \in P^\perp \setminus \{O\}} \mu(B)$$

The next lemma bounds  $\text{WF}(P)$  by the minimum weight of  $P^\perp$ .

**Lemma 6.7.** For a positive integer  $M$ , define

$$C_{s,n}(M) := \sum_{A \in (G^\vee)^{s \times n} \setminus \mathcal{B}_{s,n}(M-1)} b^{-\mu(A)} = \sum_{m=M}^{\infty} S_{s,n}(m) b^{-m}$$

and

$$C_s(M) := \sum_{m=M}^{\infty} S_s(m) b^{-m}.$$

Then we have

$$\text{WF}^n(P) = \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)} \leq C_{s,n}(\delta_{P^\perp}) \leq C_s(\delta_{P^\perp}).$$

*Proof.* The last inequality is trivial, so it suffices to prove the first inequality. Since  $P^\perp \setminus \{O\} \subset (G^\vee)^{s \times n} \setminus \mathcal{B}_{s,n}(\delta_{P^\perp} - 1)$  holds, we have

$$\begin{aligned} \text{WF}^n(P) &= \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)} \leq \sum_{A \in (G^\vee)^{s \times n} \setminus \mathcal{B}_{s,n}(\delta_{P^\perp} - 1)} b^{-\mu(A)} \\ &= C_{s,n}(\delta_{P^\perp}). \end{aligned} \quad \square$$

We shall estimate  $C_s(\lceil M' \rceil)$  ( $C$  for the Complement of the ball) for rather general real number  $M'$ : from Lemma 6.5 it follows that

$$\begin{aligned}
C_s(\lceil M' \rceil) &= \sum_{m=\lceil M' \rceil}^{\infty} S_s(m) b^{-m} \\
&\leq \sum_{m=\lceil M' \rceil}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\
&= b^{-\lceil M' \rceil} e^{2\sqrt{(b-1)s\lceil M' \rceil}} + \sum_{m=\lceil M' \rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}}. \quad (6)
\end{aligned}$$

First, we estimate the second term of the above. The function  $\exp(2\sqrt{(b-1)sm})b^{-m} = \exp(2\sqrt{(b-1)sm} - m \log b)$  is monotonically decreasing with respect to  $m$  if

$$\begin{aligned}
\frac{d}{dm} \left( 2\sqrt{(b-1)sm} - m \log b \right) &\leq 0 \iff \frac{2(b-1)s}{2\sqrt{(b-1)sm}} - \log b \leq 0 \\
&\iff \sqrt{\frac{(b-1)s}{m}} \leq \log b \\
&\iff m \geq (\log b)^{-2}(b-1)s,
\end{aligned}$$

hence we assume that  $M' \geq (\log b)^{-2}(b-1)s$ . Then, we have

$$\begin{aligned}
&\sum_{m=\lceil M' \rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\
&\leq \int_{m=\lceil M' \rceil}^{\infty} e^{-m \log b} e^{2\sqrt{(b-1)sm}} dm \\
&= \int_{m=\lceil M' \rceil}^{\infty} \exp \left( -(\log b) \left( \sqrt{m} - \frac{\sqrt{(b-1)s}}{\log b} \right)^2 + \frac{(b-1)s}{\log b} \right) dm \\
&\leq \int_{m=M'}^{\infty} \exp \left( -(\log b) \left( \sqrt{m} - \frac{\sqrt{(b-1)s}}{\log b} \right)^2 + \frac{(b-1)s}{\log b} \right) dm \\
&= \int_{x=\sqrt{M'}}^{\infty} \exp \left( -(\log b) \left( x - \frac{\sqrt{(b-1)s}}{\log b} \right)^2 + \frac{(b-1)s}{\log b} \right) 2x dx.
\end{aligned}$$

In order to bound the last integral from above, for a positive number  $c$  we assume that  $\sqrt{M'} \geq (1+c)\sqrt{(b-1)s}/\log b$  or equivalently  $M' \geq (1+c)^2(\log b)^{-2}(b-1)s$ . This assumption is stronger than the previous assumption  $M' \geq (\log b)^{-2}(b-1)s$ . Then, on the domain of integration  $x \geq \sqrt{M'} \geq (1+c)\sqrt{(b-1)s}/\log b$ , we

have  $cx \leq (1+c)(x - \sqrt{(b-1)s}/\log b)$ . Hence the estimation continues:

$$\begin{aligned}
& \sum_{m=\lceil M' \rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\
& \leq \int_{x=\sqrt{M'}}^{\infty} \exp \left( -(\log b) \left( x - \frac{\sqrt{(b-1)s}}{\log b} \right)^2 + \frac{(b-1)s}{\log b} \right) \cdot 2 \frac{1+c}{c} \left( x - \frac{\sqrt{(b-1)s}}{\log b} \right) dx \\
& = \frac{1+c}{c} \frac{1}{\log b} \left[ -\exp \left( -(\log b) \left( x - \frac{\sqrt{(b-1)s}}{\log b} \right)^2 + \frac{(b-1)s}{\log b} \right) \right]_{x=\sqrt{M'}}^{\infty} \\
& = \frac{1+c}{c} \frac{1}{\log b} \exp \left( -(\log b) \left( \sqrt{M'} - \frac{\sqrt{(b-1)s}}{\log b} \right)^2 + \frac{(b-1)s}{\log b} \right) \\
& = \frac{1+c}{c} \frac{1}{\log b} \exp(-(\log b)M' + 2\sqrt{(b-1)sM'}) \\
& = \frac{1+c}{c} \frac{1}{\log b} b^{-M'} e^{2\sqrt{(b-1)sM'}}.
\end{aligned}$$

Second, we consider the first term of (6). We have already proved that  $\exp(2\sqrt{(b-1)sm})b^{-m}$  is monotonically decreasing if  $m \geq (\log b)^{-2}(b-1)s$ , and thus the assumption  $M' \geq (\log b)^{-2}(b-1)s$  implies

$$b^{-\lceil M' \rceil} e^{2\sqrt{(b-1)s\lceil M' \rceil}} \leq b^{-M'} e^{2\sqrt{(b-1)sM'}}.$$

Therefore we have

$$\begin{aligned}
C_s(\lceil M' \rceil) & \leq b^{-\lceil M' \rceil} e^{2\sqrt{(b-1)s\lceil M' \rceil}} + \sum_{m=\lceil M' \rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\
& \leq b^{-M'} e^{2\sqrt{(b-1)sM'}} + \frac{1+c}{c} \frac{1}{\log b} b^{-M'} e^{2\sqrt{(b-1)sM'}} \\
& = \left( 1 + \frac{1+c}{c} \frac{1}{\log b} \right) b^{-M'} e^{2\sqrt{(b-1)sM'}}.
\end{aligned}$$

Now we proved:

**Proposition 6.8.** *Let  $c$  be a positive real number. Let  $M'$  be a real number with  $M' \geq (1+c)^2(\log b)^{-2}(b-1)s$ . Then we have the following bound*

$$C_{s,n}(\lceil M' \rceil) \leq C_s(\lceil M' \rceil) \leq \left( 1 + \frac{1+c}{c} \frac{1}{\log b} \right) b^{-M'} e^{2\sqrt{(b-1)sM'}}.$$

## 6.4 Existence of low-WAFOM point sets

We denote the probability of the event  $A$  by  $\text{Prob}[A]$ . Let  $p_b$  be the smallest prime factor of  $b$ . Let  $d$  be a positive integer. Choose  $d$  matrices  $B_1, \dots, B_d \in$

$G^{s \times n}$  independently and uniformly at random. Let  $P = \langle B_1, \dots, B_d \rangle \subset G^{s \times n}$  be the  $G$ -linear span of  $B_1, \dots, B_d$ , namely  $P = \{g_1 B_1 + \dots + g_d B_d \mid g_1, \dots, g_d \in G\}$  where  $g \in G$  acts on  $B = (b_{ij})$  by  $gB = (gb_{ij})$ . Note that  $|P| \leq b^d$ .

**Remark 6.9.** If  $G = \mathbb{Z}_b$ , by the theory of invariant factor decomposition, we can say that there exist matrices  $B'_1, \dots, B'_d$  such that  $P' := \langle B'_1, \dots, B'_d \rangle$  includes  $P$  and becomes a free  $\mathbb{Z}_b$ -module of rank  $d$ . Thus if  $G = \mathbb{Z}_b$ , we can replace “subgroup  $P$ ” in this subsection with a “digital net  $P$ ,” since in this subsection we consider only the existence of a subgroup which has large minimum Dick weight, and  $P \subset P'$  implies that  $\delta_{P^\perp} \leq \delta_{P'^\perp}$ .

First, we evaluate  $\text{Prob}[\text{perp}_L]$ , where we define  $\text{perp}_L$  as the event that  $B_1, \dots, B_d$  are all perpendicular to  $L \in (G^\vee)^{s \times n}$ .

**Lemma 6.10.** Let  $L \in (G^\vee)^{s \times n}$  be a nonzero matrix. Then we have  $\text{Prob}[L \perp B] \leq 1/p_b$ . Especially we have  $\text{Prob}[\text{perp}_L] \leq p_b^{-d}$ .

*Proof.* We consider the map  $(L \bullet): G^{s \times n} \rightarrow \mathbb{C}, B \mapsto L \bullet B$ . Then we have the surjective group homomorphism  $G^{s \times n} \rightarrow \text{Im}(L \bullet)$ , and thus  $|\text{Im}(L \bullet)|$  divides  $G^{s \times n}$ . Moreover, since  $L$  is nonzero,  $|\text{Im}(L \bullet)|$  is larger than 1. Hence we have  $|\text{Im}(L \bullet)| \geq p_b$ . Therefore we have  $\text{Prob}[L \perp B] = |\text{Im}(L \bullet)|^{-1} \leq 1/p_b$ , and especially we have  $\text{Prob}[\text{perp}_L] = \text{Prob}[L \perp B]^d \leq p_b^{-d}$ .  $\square$

Let  $M$  be a positive integer. We evaluate the probability of the event that  $\delta_P^\perp \geq M$ . We have

$$\begin{aligned}
\text{Prob}[\delta_P^\perp \geq M] &= 1 - \text{Prob}[\delta_P^\perp \leq M - 1] \\
&= 1 - \text{Prob}[\exists L \in \mathcal{B}_{s,n}(M-1) \setminus \{O\} \text{ s.t. } L \in P^\perp] \\
&= 1 - \text{Prob}[\exists L \in \mathcal{B}_{s,n}(M-1) \setminus \{O\} \text{ s.t. } L \perp B_1, \dots, L \perp B_d] \\
&= 1 - \text{Prob}[\cup_{L \in \mathcal{B}_{s,n}(M-1) \setminus \{O\}} \text{perp}_L] \\
&\geq 1 - \sum_{L \in \mathcal{B}_{s,n}(M-1) \setminus \{O\}} \text{Prob}[\text{perp}_L] \\
&\geq 1 - (\text{vol}_{s,n}(M-1) - 1) \cdot p_b^{-d} \\
&> 1 - \text{vol}_{s,n}(M-1) \cdot p_b^{-d}.
\end{aligned}$$

This shows:

**Proposition 6.11.** If  $\text{vol}_{s,n}(M-1) \leq p_b^d$  holds, then there exists a subgroup  $P \subset G^{s \times n}$  with  $|P| \leq b^d$  satisfying  $\delta_{P^\perp} \geq M$ .

By Lemma 6.4, the condition of this proposition is satisfied if it holds that

$$e^{2\sqrt{(b-1)s(M-1)}} \leq p_b^d \iff M \leq \frac{(\log p_b)^2 d^2}{4(b-1)s} + 1.$$

Therefore we have the following sufficient condition on the existence of  $M$ .

**Proposition 6.12.** *If  $M \leq (\log p_b)^2 d^2 / (4(b-1)s) + 1$  holds, then Inequality (6.4) is satisfied, and hence there exists a subgroup  $P \subset G^{s \times n}$  with  $|P| \leq b^d$  satisfying  $\delta_{P^\perp} \geq M$ .*

From now on, we define  $\alpha_b := (\log p_b)/2$  and  $M' := A^2 d^2 / ((b-1)s)$  where  $A \leq \alpha_b$  and we take  $M$  to be  $\lfloor M' + 1 \rfloor$  so that  $P$  with  $|P| \leq b^d$  and  $\delta_{P^\perp} \geq M$  exists. Then, by Proposition 6.8, we have the following upper bound of  $\text{WF}(P)$ :

**Proposition 6.13.** *Let  $\alpha_b := (\log p_b)/2$ . Take a real number  $A$  with  $A \leq \alpha_b$  and an arbitrary real number  $c > 0$ . Then for any positive integers  $s, n$ , and  $d \geq (1+c)(b-1)s/(A \log b)$ , there exists a subgroup  $P \subset G^{s \times n}$  with  $|P| \leq b^d$  satisfying*

$$\text{WF}^n(P) \leq \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-A^2 d^2 / ((b-1)s)} e^{2Ad}.$$

Moreover, if  $n \geq A^2 d^2 / ((b-1)s)$ , the above  $P$  satisfies that

$$\text{WF}^\infty(P_\infty) \leq \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-A^2 d^2 / ((b-1)s)} e^{2Ad}.$$

*Proof.* define  $M' := A^2 d^2 / ((b-1)s)$  and  $M := \lfloor M' + 1 \rfloor$ . By Proposition 6.12, there exists a subgroup  $P \subset \mathbb{Z}_b^{s \times n}$  with  $|P| \leq b^d$  and  $\delta_{P^\perp} \geq M$ . For this  $P$ , from Proposition 6.8 we have

$$\begin{aligned} \text{WF}(P) &\leq C_s(M) \\ &\leq C_s(\lceil M' \rceil) \\ &\leq \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-M'} e^{2\sqrt{(b-1)sM'}} \\ &= \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-A^2 d^2 / ((b-1)s)} e^{2Ad}, \end{aligned}$$

and this proves the first statement.

If we assume that  $n \geq M'$ , we have  $\delta_{P_\infty^\perp} \geq \min(\delta_{P^\perp}, n+1) \geq M$ , and thus we can carry out the above calculation with replacing  $P$  by  $P_\infty$ . This proves the second statement.  $\square$

In particular, take  $A = \alpha_b$  and we have the next theorem.

**Theorem 6.14.** *Let  $\alpha_b := (\log p_b)/2$  and take an arbitrary real number  $c > 0$ . Then for any  $s, n$ , and  $d \geq (1+c)(b-1)s/(\alpha_b \log b)$ , there exists a subgroup  $P \subset G^{s \times n}$  with  $|P| \leq b^d$  satisfying*

$$\text{WF}(P) \leq \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-\alpha_b^2 d^2 / ((b-1)s)} e^{2\alpha_b d}.$$

Applying Theorem 6.14 to the case  $G = \mathbb{F}_2$ , we can improve [9, Theorem 2 and Remark 5].

**Corollary 6.15.** *Let  $\alpha := \alpha_2 = (\log 2)/2$  and take an arbitrary real number  $c > 0$ . Then for any  $n$  and  $d \geq (1+c)s/(\alpha \log 2)$ , there exists a linear subspace  $P \subset \mathbb{F}_2^{s \times n}$  with  $\dim P \leq d$  satisfying*

$$\text{WF}(P) \leq \left(1 + \frac{1+c}{c} \frac{1}{\log 2}\right) 2^{-\alpha^2 d^2/s} e^{2\alpha d}.$$

**Remark 6.16.** *Suzuki [13] proved that the construction of higher order digital net on  $\mathbb{F}_p$  given in [1] combined with some Niederreiter-Xing point sets [11] yields an explicit construction of low-WAFOM point sets, whose order of WAFOM is almost the same with the order obtained in this paper.*

**Remark 6.17.** *Theorem 6.14 and Corollary 6.15 holds in the  $n = \infty$  case. This is the consequence of the second statement of Proposition 6.13.*

## 6.5 A lower bound of WAFOM

In this subsection, we show a lower bound on  $\text{WAFOM}(P)$ , as a generalization of [14]. The next lemma gives an upper bound on minimum Dick weight of  $P^\perp$  for given  $P \subset G^{s \times n}$ , which implies a lower bound of  $\text{WAFOM}(P)$ .

**Lemma 6.18.** *Suppose that  $s$  and  $n$  are positive integers. Let  $P \subset G^{s \times n}$  be a subgroup with  $|P| \leq b^d$ . Let  $q, r$  be nonnegative integers which satisfy  $d = qs + r$  and  $0 \leq r < s$ . Then we have the following:*

1.  $\delta_{P^\perp} \leq sq(q+1)/2 + (q+1)(r+1) \leq d^2/2s + 3d/2 + s$ .
2. *Let  $C$  be an arbitrary positive real number greater than  $1/2$ . If  $d/s \geq (\sqrt{C} + 1/16 + 3/4)/(C - 1/2)$  holds, then we have  $\delta_{P^\perp} \leq Cd^2/s$ .*

*Proof.* We define a subgroup  $Q := \{A = (a_{ij}) \in (G^\vee)^{s \times n} \mid a_{ij} = 0 \text{ if } (q+2 \leq j \leq n) \text{ or } (j = q+1 \text{ and } r+2 \leq i \leq s)\}$ . We have  $|Q| = b^{qs+r+1} = b^{d+1}$ . There is a  $\mathbb{Z}$ -module isomorphism  $P^\perp/(P^\perp \cap Q) \simeq (P^\perp + Q)/Q$ , and thus we have

$$|P^\perp \cap Q| = \frac{|P^\perp| \cdot |Q|}{|P^\perp + Q|} \geq \frac{b^{sn-d} \cdot b^{d+1}}{|(G^\vee)^{s \times n}|} = b,$$

especially there exists a non-zero matrix  $A' \in (P^\perp \cap Q)$ . Therefore we have

$$\delta_{P^\perp} \leq \mu(A') \leq \max\{\mu(A) \mid A = (a_{ij}) \in Q\} = sq(q+1)/2 + (q+1)(r+1),$$

where the last equality holds if the components of  $A$  is as follows:

$$\begin{cases} a_{ij} = 0 & \text{if } (q+2 \leq j \leq n) \text{ or } (j = q+1 \text{ and } r+2 \leq i \leq s) \\ a_{ij} \neq 0 & \text{if } (1 \leq j \leq q) \text{ or } (j = q+1 \text{ and } 1 \leq i \leq r+1) \end{cases}.$$

In particular, since  $q \leq d/s$  and  $r+1 \leq s$ , we have

$$\begin{aligned} \delta_{P^\perp} &\leq sq(q+1)/2 + (q+1)(r+1) \\ &\leq \frac{d}{2} \left(\frac{d}{s} + 1\right) + \left(\frac{d}{s} + 1\right)s = \frac{d^2}{s} \left(\frac{1}{2} + \frac{3s}{2d} + \frac{s^2}{d^2}\right), \end{aligned}$$

which proves the first statement.

Let  $C$  be a real number greater than  $1/2$  and we assume  $d/s \geq (\sqrt{C+1/16} + 3/4)/(C-1/2)$ . Then we have  $1/2 + 3s/2d + s^2/d^2 \leq C$ . Thus we obtain

$$\delta_{P^\perp} \leq \frac{d^2}{s} \left( \frac{1}{2} + \frac{3s}{2d} + \frac{s^2}{d^2} \right) \leq Cd^2/s,$$

which proves the second statement.  $\square$

The above lemma gives a lower bound of  $\text{WF}(P)$ .

**Theorem 6.19.** *Suppose that  $s$  and  $n$  are positive integers. Let  $G$  be a finite abelian group with  $b \geq 2$  elements. Let  $P \subset G^{s \times n}$  be a subgroup with  $|P| \leq b^d$ . Let  $C$  be an arbitrary positive real number greater than  $1/2$ . If  $d/s \geq (\sqrt{C+1/16} + 3/4)/(C-1/2)$  holds, then we have*

$$\text{WF}^n(P) \geq b^{-Cd^2/s}.$$

*Proof.*

$$\text{WF}^n(P) = \sum_{A \in P^\perp \setminus \{O\}} b^{-\mu(A)} \geq b^{-\delta_{P^\perp}} \geq b^{-Cd^2/s}.$$

$\square$

**Remark 6.20.** *Propositions in this subsection follow in the case of  $n = \infty$ . Assume that  $n = \infty$  and  $P \subset G^{s \times \mathbb{N}}$  is a subgroup. We fix an integer  $m$  such that  $|\text{pr}_m(P)| = |P|$ . Since  $|P|$  is finite, such  $m$  exists. Then we have  $\delta_{P^\perp} \leq \delta_{\text{pr}_m(P)^\perp}$ , and thus the infinite case reduces to the finite case.*

## 6.6 Order of WAFOM

In this subsection, we consider the order of  $\text{WF}(P)$  where  $P$  is a subgroup of  $G^{s \times n}$  with  $|P| = b^d$ .

We fix the base  $b$ . Let  $D := \alpha_b = (\log p_b)/2$ . We fix a positive integer  $E$  satisfying  $E > (b-1)/(D \log b)$ . Let  $c$  be the real number such that  $E = (1+c)(b-1)/(D \log b)$  (by the assumption that  $E > (b-1)/(D \log b)$ ,  $c$  is positive). Note that  $c$ ,  $D$  and  $E$  depend only on  $b$ .

We assume that  $d/s \geq E$ . Then, by Proposition 6.13, there exists a subgroup  $P \subset G^{s \times n}$  with  $|P| \leq b^d$  satisfying

$$\text{WF}^n(P) \leq \left( 1 + \frac{1+c}{c} \frac{1}{\log b} \right) b^{-D^2 d^2 / ((b-1)s)} e^{2Dd}.$$

Moreover, by Theorem 6.19, for every  $P$  with  $|P| \leq b^d$  we have  $\text{WF}^n(P) \geq b^{-Cd^2/s}$  where  $C = (1/2 + 3/(2E) + 1/E^2)$ . Thus we have the following lemma.

**Lemma 6.21.** *If  $d/s \geq E$ , we have*

$$\begin{aligned} -Cd^2/s &\leq \min\{\log_b(\text{WF}^n(P)) \mid P \subset G^{s \times n} \text{ subgroup, } |P| \leq b^d\} \\ &\leq -D^2 d^2 / ((b-1)s) + 2Dd / \log b + \log_b \left( 1 + \frac{1+c}{c} \frac{1}{\log b} \right). \end{aligned}$$

Especially, let  $N = b^d$  and we have the following.

**Theorem 6.22.** *Let  $G$  be a finite abelian group with  $|G| = b$ . Let  $P \subset G^{s \times n}$  be a subgroup with  $|P| \leq N$ . Let  $c, C, D$ , and  $E$  are constants as Lemma 6.21, which depend only on  $b$ . Suppose that  $(\log N)/s \geq E$ . Then we have*

$$\begin{aligned} N^{-C(\log N)/s} &\leq \min\{\text{WF}^n(P) \mid P \subset G^{s \times n} \text{ subgroup}, |P| \leq N\} \\ &\leq \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) N^{-D^2(\log N)/((\log b)(b-1)s) + 2D/\log b}. \end{aligned}$$

**Remark 6.23.** *Considering Remark 6.17 and Remark 6.20, we can see that propositions in this subsection follows in the case of  $n = \infty$ .*

## Acknowledgements

The works of the author were supported by the Program for Leading Graduate Schools, MEXT, Japan.

## References

- [1] Josef Dick. Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order. *SIAM J. Numer. Anal.*, 46(3):1519–1553, 2008.
- [2] Josef Dick. The decay of the Walsh coefficients of smooth functions. *Bull. Aust. Math. Soc.*, 80(3):430–453, 2009.
- [3] Josef Dick and Makoto Matsumoto. On the Fast Computation of the Weight Enumerator Polynomial and the  $t$  Value of Digital Nets over Finite Abelian Groups. *SIAM J. Discrete Math.*, 27(3):1335–1359, 2013.
- [4] Josef Dick and Friedrich Pillichshammer. *Digital nets and sequences: Discrepancy theory and quasi-Monte Carlo integration*. Cambridge University Press, Cambridge, 2010.
- [5] Gerhard Larcher, Harald Niederreiter, and Wolfgang Ch. Schmid. Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration. *Monatsh. Math.*, 121(3):231–253, 1996.
- [6] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I*. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.
- [7] Jiří Matoušek and Jaroslav Nešetřil. *Invitation to discrete mathematics*. The Clarendon Press Oxford University Press, New York, 1998.
- [8] Makoto Matsumoto, Mutsuo Saito, and Kyle Matoba. A computable figure of merit for quasi-Monte Carlo point sets. to appear in *Math. Comp.*



- [9] Makoto Matsumoto and Takehito Yoshiki. Existence of higher order convergent quasi-Monte Carlo rules via Walsh figure of merit. In *Monte Carlo and quasi-Monte Carlo methods 2012*, pages 569–579. Springer, Berlin, 2013.
- [10] Harald Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.
- [11] Harald Niederreiter and Chaoping Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2001.
- [12] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
- [13] Kosuke Suzuki. An explicit construction of point sets with large minimum Dick weight. to appear in J. Complexity.
- [14] Takehito Yoshiki. A Lower Bound on WAFOM. preprint.